CHAPTER 2

Catalyst 5000 Series Switch Workgroup MIBs

This chapter contains descriptions of the groups and variables used within the Cisco Workgroup MIB file, the CISCO-STACK-MIB.

For information regarding other MIBs supported by the Catalyst 5000 series switch, refer to the *Cisco Management Information Base (MIB) User Quick Reference* publication.

Note Default values are included where available.

This chapter includes the following sections:

- System Group
- Chassis Group
- Module Group
- Port Group
- Trivial File Transfer Protocol Group
- Monitor Group
- VLAN Group
- Security Group
- Multicast Group
- Domain Naming System Group
- System Log Information Group

- Network Time Protocol Group
- Terminal Access Controller Access Control System Group
- IP Permit List Group
- Port Channel Group
- Spanning-Tree Status Group

Note In this document, reference to the Catalyst 5000 series switches refers specifically to the Catalyst 5000, Catalyst 5002, and Catalyst 5500 switches.

System Group

The System group manages and controls system-wide functionality of the Catalyst 5000 series switch products.

Implementation of the System group is mandatory for all Cisco Workgroup Stack products.

sysMgmtType (systemGrp 1)

Specifies the type of network management running on this system.

Syntax: Integer {

other (1)	None of the following
snmpV1 (2)	SNMP
smux (3)	SNMP MUX subagent
snmpV2V1 (4)	Bilingual SNMP, Version 2 and 1

Access: Read-only

sysIpAddr (systemGrp 2)

Specifies the IP address.

Syntax: IpAddress

Access: Read-write

sysNetMask (systemGrp 3)

Specifies the subnet mask.

Syntax: IpAddress

Access: Read-write

sysBroadcast (systemGrp 4)

Specifies the broadcast address.

Syntax: IpAddress

Access: Read-write

sysTrapReceiverTable (systemGrp 5)

Contains a list of Network Management Station addresses that should receive trap messages from this system when an exception condition occurs and includes the following variables: *sysTrapReceiverType*, *sysTrapReceiverAddr*, and *sysTrapReceiverComm.*

Syntax: SEQUENCE OF SysTrapReceiverEntry

Access: Not accessible

sysTrapReceiverEntry (sysTrapReceiverTable 1)

Provides a trap receiver table entry.

Syntax: SysTrapReceiverEntry

Access: Not accessible

sysTrapReceiverType (sysTrapReceiverEntry 1)

Adds or deletes an entry from the sysTrapReceiverTable.

Syntax: Integer {

valid (1) Add this entry

invalid (2) Remove this entry

Access: Read-write

sysTrapReceiverAddr (sysTrapReceiverEntry 2)

Specifies the IP address for the trap receiver.

Syntax: IpAddress

Access: Read-only

sysTrapReceiverComm (sysTrapReceiverEntry 3)

Provides a community string used for trap messages to this trap receiver.

Syntax: DisplayString (SIZE 0..20)

Access: Read-write

End of Table

Note systemGrp 6 and systemGrp 7 are not used.

sysTraffic (systemGrp 8)

Specifies the traffic meter value; for example, the percentage of bandwidth utilization for the previous polling interval.

Syntax: Integer (0..100)

Access: Read-only

sysReset (systemGrp 9)

Provides a method of resetting the control logic of all modules in the system.

Syntax: Integer {

other (1)	None of the following
reset (2)	Resetting

Access: Read-write

sysBaudRate (systemGrp 10)

Specifies the baud rate in bits per second (bps) of the RS-232 port.

Syntax: Integer {

b600 (600])	600 bps
b1200 (1200)	1200 bps
b2400 (2400)	2400 bps
b4800 (4800)	4800 bps
b9600 (9600)	9600 bps (default)
b19200 (19200)	19200 bps
b38400 (38400)	38400 bps

Access: Read-write

Note systemGrp 11 is not used.

sysClearMacTime (systemGrp 12)

Specifies the time (in hundredths of a second) since the Media Access Control (MAC) counters were last cleared. Writing 0 causes the MAC counters to be cleared.

Syntax: TimeTicks

Access: Read-write

sysClearPortTime (systemGrp 13)

Specifies the time (in hundredths of a second) since the port counters were last cleared. Writing 0 clears the port counters.

Syntax: TimeTicks

Access: Read-write

Note systemGrp 14 is not used.

sysEnableModem (systemGrp 15)

Enables or disables the RS-232 port modem control lines.

Syntax: Integer {

enabled (1)	RS-232 port modem control lines are enabled.
disabled (2)	RS-232 port modem control lines are disabled (default).

Access: Read-write

sysEnableRedirects (systemGrp 16)

Specifies whether the system can send or receive Internet Control Message Protocol (ICMP) redirect messages.

Syntax: Integer {

enabled (1) The system can send or receive ICMP redirect messages.

disabled (2) The system cannot send or receive ICMP redirect messages.

Access: Read-write

sysEnableRmon (systemGrp 17)

Specifies whether the SNMP agent supports the Remote Monitoring (RMON) MIB.

Syntax: Integer {

enabled (1) The SNMP agent supports the RMON MIB (default).

disabled (2) The SNMP agent does not support the RMON MIB.

Access: Read-write

sysArpAgingTime (systemGrp 18)

Indicates the aging time of the ARP table.

Syntax: Integer (0..1000000) (default is 1200)

Access: Read-write

sysTrafficPeak (systemGrp 19)

Indicates the peak traffic meter value since the last time port counters were cleared or the system started (see *sysClearPortTime*).

Syntax: Integer (0..100)

Access: Read-only

sysTrafficPeakTime (systemGrp 20)

Indicates the time (in hundredths of a second) since the peak traffic meter value occurred.

Syntax: TimeTicks

Access: Read-only

sysCommunityRwa (systemGrp 21)

When an SNMP message is received, the community string in the message is compared to the sysCommunityRwa string first. If it matches, read-write access is granted to all items in the MIB. If it does not match, the sysCommunityRw string is then compared.

Note This item is only accessible when using the community string defined in sysCommunityRwa.

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

sysCommunityRw (systemGrp 22)

If the community string in the received SNMP message does not match the sysCommunityRwa string, the message is then compared with the sysCommunityRw string. If it matches, read-write access is granted to all items in the MIB except for restricted items such as community strings. (Restricted items appear empty when read and return a "no such name" error when an attempt is made to write them.) If it does not match, the sysCommunityRo string is then compared.

Note This item is only accessible when using the community string defined in sysCommunityRwa.

---

sysCommunityRw (systemGrp 22)—Continued

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

sysCommunityRo (systemGrp 23)

If the community string in the received SNMP message does not match the sysCommunityRw string, the message is then compared with the sysCommunityRo string. If it matches, read-only access is granted to all items in the MIB except for restricted items such as community strings. (Restricted items appear empty when read.) If it does not match, access is denied, no response is sent back to the SNMP requestor, and an SNMP trap is sent to the SNMP trap receivers (if configured).

Note This item is only accessible when using the community string defined in sysCommunityRwa.

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

sysEnableChassisTraps (systemGrp 24)

Specifies whether the chassisAlarmOn and chassisAlarmOff traps in this MIB should be generated.

Syntax: Integer {

enabled (1)	chassisAlarmOn and chassisAlarmOff traps in this MIB are generated.
disabled (2)	chassisAlarmOn and chassisAlarmOff traps in this MIB are not generated (default).

Access: Read-write

sysEnableModuleTraps (systemGrp 25)

Specifies whether the moduleUp and moduleDown traps in this MIB should be generated.

Syntax: Integer {

- enabled (1) — moduleUp and moduleDown traps in this MIB are generated.
- disabled (2) — moduleUp and moduleDown traps in this MIB are not generated (default).

Access: Read-write

sysEnableBridgeTraps (systemGrp 26)

Specifies whether the newRoot and topologyChange traps in the BRIDGE-MIB (RFC 1495) should be generated.

Syntax: Integer {

- enabled (1) — newRoot and topologyChange traps in the BRIDGE-MIB (RFC 1495) are generated.
- disabled (2) — newRoot and topologyChange traps in the BRIDGE-MIB (RFC 1495) are not generated (default).

Access: Read-write

sysIpVlan (systemGrp 27)

Specifies this entity's IP address virtual LAN (VLAN) association.

Syntax: Integer (0..1023)

Access: Read-write

sysConfigChangeTime (systemGrp 28)

Indicates the time (in hundredths of a second) since the configuration of the system was last changed.

Syntax: TimeTicks

Access: Read-only

sysEnableRepeaterTraps (systemGrp 29)

Specifies whether the traps in the REPEATER-MIB (RFC 1516) should be generated.

Syntax: Integer {

enabled (1)	The traps in the REPEATER-MIB (RFC 1516) are to be generated.
disabled (2)	The traps in the REPEATER-MIB (RFC 1516) are not to be generated (default).

Access: Read-write

sysBannerMotd (systemGrp 30)

Displays the message of the day banner on the command-line interface before log in.

Syntax: DisplayString (SIZE (0..255))

Access: Read-write

sysEnableIpPermitTraps (systemGrp 31)

Indicates whether the IP permit traps in this MIB should be generated.

Syntax: Integer {

enabled (1)	The traps in this MIB are to be generated.
disabled (2)	The traps in this MIB are not to be generated (default).

Access: Read-write

Chassis Group

The Chassis group manages and controls the various functions of the chassis components, such as the power supply type and status, number of slots available for plug-in modules, and chassis model number.

Implementation of the Chassis group is mandatory for all Cisco Workgroup Stack products.

chassisSysType (chassisGrp 1)

Indicates the chassis system type.

Syntax: Integer {

other (1)	None of the following
wsc1000 (3)	2+8 port CDDI concentrator
wsc1001 (4)	2+8 port CDDI concentrator
wsc1100 (5)	2+16 port FDDI/CDDI concentrator
wsc5000 (6)	5-slot switch
wsc2900 (7)	Closed 2-slot switch
wsc5500 (8)	13-slot switch
wsc5002 (9)	2-slot switch
wsc1200 (11)	2+8 port FDDI/Ethernet switch
wsc1400 (12)	2-slot FDDI/CDDI concentrator

Access: Read-only

chassisBkplType (chassisGrp 2)

Indicates the chassis backplane type.

Syntax: Integer {

other (1)	None of the following
fddi (2)	fddi
fddiEthernet (3)	fddi and ethernet
giga (4)	gigabit packet switch
giga3 (5)	3.6 gigabit switch
giga3E (6)	3.6 gigabit switch enhanced

Access: Read-only

chassisPs1Type (chassisGrp 3)

Indicates the type of power supply number 1.

Syntax: Integer {

other (1)	None of the following
none (2)	No power supply
w50 (3)	50 watt supply
w200 (4)	200 watt supply
w600 (5)	600 watt supply
w80 (6)	80 watt supply
w130 (7)	130 watt supply
wsc5008 (8)	350 watt supply
wsc5008a (9)	350 watt supply
w175 (10)	175 watt supply
wsc5068 (11)	350 watt supply (DC)

chassisPs1Type (chassisGrp 3)—Continued

wsc5508 (12)	1100 watt supply
wsc5568 (13)	1100 watt supply (DC)
wsc5508a (14)	1200 watt supply
w155 (15)	155 watt supply
w155pfc (16)	155 watt supply w/PFC
w155dc (17)	155 watt supply (DC)

Access: Read-only

chassisPs1Status (chassisGrp 4)

Provides the status of power supply number 1. If the status is “not ok,” the value of chassisPs1TestResult gives more detailed information about the power supply’s failure condition(s).

Syntax: Integer {

other (1)	None of the following
ok (2)	Status ok
minorFault (3)	Minor problem
majorFault (4)	Major problem

Access: Read-only

chassisPs1TestResult (chassisGrp 5)

Provides the test result for power supply number 1. A zero indicates that the supply passed all tests. Bits set in the result indicate error conditions.

Syntax: Integer (0..65535)

Access: Read-only

chassisPs2Type (chassisGrp 6)

Indicates the type of power supply number 2.

Syntax: Integer {

other (1)	None of the following
none (2)	No power supply
w50 (3)	50 watt supply
w200 (4)	200 watt supply
w600 (5)	600 watt supply
w80 (6)	80 watt supply
w130 (7)	130 watt supply
wsc5008 (8)	350 watt supply
wsc5008a (9)	350 watt supply
w175 (10)	175 watt supply
wsc5068 (11)	350 watt supply (DC)
wsc5508 (12)	1100 watt supply
wsc5568 (13)	1100 watt supply (DC)
wsc5508a (14)	1200 watt supply
w155 (15)	155 watt supply
w155pfc (16)	155 watt supply w/PFC
w155dc (17)	155 watt supply (DC)

Access: Read-only

chassisPs2Status (chassisGrp 7)

Provides the status of power supply number 2. If the status is “not ok,” the value of chassisPs2TestResult gives more detailed information about the power supply’s failure condition(s).

Syntax: Integer {

other (1)	None of the following
ok (2)	Status satisfactory
minorFault (3)	Minor problem
majorFault (4)	Major problem

Access: Read-only

chassisPs2TestResult (chassisGrp 8)

Provides the test result for power supply number 2. A zero indicates that the supply passed all tests. Bits set in the result indicate error conditions.

Syntax: Integer (0..65535)

Access: Read-only

chassisFanStatus (chassisGrp 9)

Provides the status of the chassis fan. If the status is “not ok,” the value of chassisFanTestResult gives more detailed information about the fan’s failure condition(s).

Syntax: Integer {

other (1)	None of the following
ok (2)	Status satisfactory
minorFault (3)	Minor problem
majorFault (4)	Major problem

Access: Read-only

chassisFanTestResult (chassisGrp 10)

Provides the test result for the chassis fan. A zero indicates that the fan passed all tests. Bits set in the result indicate error conditions.

Syntax: Integer (0..65535)

Access: Read-only

chassisMinorAlarm (chassisGrp 11)

Provides the chassis minor alarm status.

Syntax: Integer {

off (1)	No chassis minor alarm has been detected.
on (2)	A chassis minor alarm has been detected.

Access: Read-only

chassisMajorAlarm (chassisGrp 12)

Provides the chassis major alarm status.

Syntax: Integer {

off (1)	No chassis major alarm has been detected.
on (2)	A chassis major alarm has been detected.

Access: Read-only

chassisTempAlarm (chassisGrp 13)

Provides the chassis temperature alarm status.

Syntax: Integer {

off (1)	Temperature within normal range
on (2)	Temperature too high
critical (3)	Critical temperature, system shutdown imminent

Access: Read-only

chassisNumSlots (chassisGrp 14)

Indicates the number of slots in the chassis available for plug-in modules.

Syntax: Integer (1..16)

Access: Read-only

chassisSlotConfig (chassisGrp 15)

Indicates the slots in the chassis with modules inserted. The syntax is an integer value with bits set to indicate configured modules. It can be interpreted as a sum of f(x) as x goes from 1 to the number of slots, where f(x) = 0 for no module inserted and f(x) = exp(2, x-1) for a module inserted.

Syntax: Integer (0..65535)

Access: Read-only

chassisModel (chassisGrp 16)

Indicates the manufacturer's model number for the chassis.

Syntax: DisplayString (SIZE (0..8))

Access: Read-only

chassisSerialNumber (chassisGrp 17)

Indicates the serial number of the chassis.

Syntax: Integer (0..999999999)

Access: Read-only

Module Group

The Module group provides module descriptions, such as the module type, firmware version, hardware version, serial number, operational status, and self-test results.

Implementation of the Module group is mandatory for all Cisco Workgroup Stack products.

moduleTable (moduleGrp 1)

Contains a list of module entries. The number of entries is given by the value of chassisNumSlots and includes the following variables: *moduleIndex, moduleType, moduleSerialNumber, moduleHwHiVersion, moduleHwLoVersion, moduleFwHiVersion, moduleFwLoVersion, moduleSwHiVersion, moduleSwLoVersion, moduleStatus, moduleTestResult, moduleAction, moduleName, moduleNumPorts, modulePortStatus, moduleSubType, moduleModel, moduleHwVersion, moduleFwVersion, moduleSwVersion,* and *moduleStandbyStatus, moduleIPaddress, moduleIPvlan.*

Syntax: SEQUENCE OF ModuleEntry

Access: Not accessible

moduleEntry (moduleTable 1)

Provides information about one module in a slot of the chassis.

Syntax: ModuleEntry

Access: Not accessible

moduleIndex (moduleEntry 1)

Indicates a unique value for each module within the chassis. This value is determined by the chassis slot number where the module is inserted. Valid entries are 1 to the value of chassisNumSlots.

Syntax: Integer (1..16)

Access: Read-only

moduleType (moduleEntry 2)

Indicates the type of module.

Syntax: Integer {

other (1)	None of the following
empty (2	Nothing installed
wsc1000 (3)	2+8 port CDDI concentrator
wsc1001 (4)	2+8 port FDDI C concentrator
wsc1100 (5)	2+16 port FDDI/CDDI C concentrator
wsc1200 (11)	2+8 port FDDI/Ethernet switch
wsc1400 (12)	2-slot FDDI/CDDI C concentrator
wsx5009 (23)	Supervisor module, 100BaseTX (RJ-45/MII)
wsx5013 (24)	24-port 10BaseT (RJ-45 connector)
wsx5011 (25)	12-port 10BaseFL multimode (ST connector)
wsx5010 (26)	24-port 10BaseT (telco connector)
wsx5113 (27)	12-port 100BaseTX (RJ-45 connector)
wsx5101 (28)	Dual attach multimode FDDI (MIC connector)
wsx5103 (29)	Dual attach CDDI (RJ-45 connector)
wsx5104 (30)	Dual attach single-mode FDDI (ST connector)
wsx5105 (31)	Dual attach multimode FDDI (SC connector)
wsx5155 (32)	1-port multimode OC-3 ATM (SC connector)
wsx5154 (33)	1-port single-mode OC-3 ATM (SC connector)
wsx5153 (34)	1-port UTP OC-3 ATM (RJ-45 connector)
wsx5111 (35)	12-port 100BaseFX multimode (SC connector)
wsx5213 (36)	12-port 10/100BaseTX (RJ-45 connector)
wsx5020 (37)	48-port 4-segment 10BaseT (telco connector)

moduleType (moduleEntry 2)—Continued

wsx5006 (38)	Supervisor module, 100BaseFX multimode (SC connector)
wsx5005 (39)	Supervisor module, 100BaseFX single-mode (SC connector)
wsx5509 (40)	Supervisor module II, 100BaseTX (RJ-45/MII)
wsx5506 (41)	Supervisor module II, 100BaseFX multimode (SC)
wsx5505 (42	Supervisor module II, 100BaseFX single-mode (SC)
wsx5156 (43)	2-port UTP OC-3 ATM (RJ-45 connector)
wsx5157 (44)	2-port single-mode OC-3 ATM (SC connector)
wsx5158 (45)	2-port multimode OC-3 ATM (SC connector)
wsx5114 (47)	6-port single-mode, 6-port MM 100BaseFX (SC connector)
wsx5223 (48)	24-port 3-segment 100BaseTX (RJ-45 connector)
wsx5224 (49)	24-port 10/100BaseTX (RJ-45 connector)
wsx5012 (50)	48-port 10BaseT (telco connector)
wsx5302 (52)	VLAN router module (for the Catalyst 5000)
wsx5213a (53)	12-port 10/100BaseTX (RJ-45 connector)
wsx5201 (55)	12 port 100BaseFX multimode (SC connector)
wsx5203 (56)	12 port 10/100BaseTX (RJ-45 connector)

Access: Read-only

moduleSerialNumber (moduleEntry 3)

Provides the serial number of the module.

Syntax: Integer (0..999999999)

Access: Read-only

moduleHwHiVersion (moduleEntry 4)

Provides the high part of the hardware version of the module. For example, if the hardware version is 3.1, the value of moduleHwHiVersion is 3.

Syntax: Integer (0..65535)

Access: Read-only

moduleHwLoVersion (moduleEntry 5)

Provides the low part of the hardware version of the module. For example, if the hardware version is 3.1, the value of moduleHwLoVersion is 1.

Syntax: Integer (0..65535)

Access: Read-only

moduleFwHiVersion (moduleEntry 6)

Provides the high part of the firmware version number. For example, if the firmware version is 3.1, the value of moduleFwHiVersion is 3.

Syntax: Integer (0..65535)

Access: Read-only

moduleFwLoVersion (moduleEntry 7)

Provides the low part of the firmware version number. For example, if the firmware version is 3.1, the value of moduleFwLoVersion is 1.

Syntax: Integer (0..65535)

Access: Read-only

moduleSwHiVersion (moduleEntry 8)

Provides the high part of the software version number. For example, if the software version is 3.1, the value of moduleSwHiVersion is 3.

Syntax: Integer (0..65535)

Access: Read-only

moduleSwLoVersion (moduleEntry 9)

Provides the low part of the software version number. For example, if the software version is 3.1, the value of moduleSwLoVersion is 1.

Syntax: Integer (0..65535)

Access: Read-only

moduleStatus (moduleEntry 10)

Provides the operational status of the module. If the status is "not ok," the value of moduleTestResult gives more detailed information about the module's failure condition(s).

Syntax: Integer {

other (1)	None of the following
ok (2)	Status satisfactory
minorFault (3)	Minor problem. A minor problem is defined as a module that is under startup diagnostics, not online, or is disabled.
majorFault (4)	Major problem. A major problem is defined as a module not running (for example, no CPU), or a major component diagnostic failure has occurred, so that the module is not usable.

Access: Read-only

moduleTestResult (moduleEntry 11)

Provides the results of the module's self-test. A zero indicates that the module passed all tests. Bits set in the result indicate error conditions.

Syntax: Integer (0..65535)

Access: Read-only

moduleAction (moduleEntry 12)

Specifies that this object, when read, returns one of the following results:

other (1)	Module is permanently enabled.
enable (3)	Module is currently enabled.
disable (4)	Module is currently disabled.

Setting this object to one of the acceptable values gives the following results; setting this object to any other value results in an error:

Syntax: Integer {

other (1)	Gives an error.
reset (2)	Resets the module's control logic. (If configuring the VLAN router module [for the Catalyst 5000], always set to reset [2]; otherwise an error is given.)
enable (3)	If the module status is configurable, enables the module, or else gives error.
disable (4)	If the module status is configurable, disables the module, or else gives error.

Access: Read-write

moduleName (moduleEntry 13)

Specifies the descriptive string used by the network administrator to name the module.

Syntax: DisplayString (SIZE (0..20)

Access: Read-write

moduleNumPorts (moduleEntry 14)

Indicates the number of ports supported by the module.

Syntax: Integer (0..255)

Access: Read-only

modulePortStatus (moduleEntry 15)

Specifies a series of bytes containing status information about the module and each of the ports on the module. The first byte contains the status for the module (same value as moduleStatus), and subsequent bytes contain status for the first through the last ports on the module (same value as portOperStatus).

Syntax: OCTET STRING (SIZE (0..50))

Access: Read-only

moduleSubType (moduleEntry 16)

Indicates the type of daughterboard attached to this module.

Syntax: Integer {

other (1)	None of the following
empty (2)	Nothing installed
wsf5510 (3)	EARL 1

moduleSubType (moduleEntry 16)—Continued

wsf5511 (4) EARL 1+

wsf5512 (5) EARL 2

wsx5304 (6) VIP II carrier

Access: Read-only

moduleModel (moduleEntry 17)

Indicates the manufacturer's model number for the module.

Syntax: DisplayString (SIZE (0..8))

Access: Read-only

moduleHwVersion (moduleEntry 18)

Indicates the hardware version of the module.

Syntax: DisplayString (SIZE (0..12))

Access: Read-only

moduleFwVersion (moduleEntry 19)

Indicates the firmware version of the module.

Syntax: DisplayString (SIZE (0..12))

Access: Read-only

moduleSwVersion (moduleEntry 20)

Indicates the software version of the module.

Syntax: DisplayString (SIZE (0..20))

Access: Read-only

moduleStandbyStatus (moduleEntry 21)

Provides the status of a redundant module.

Syntax: Integer {

other (1)	None of the following.
active (2)	The redundant module is active.
standby (3)	The redundant module is in standby mode.
error (4)	The redundant module is in error.

Access: Read-only

moduleIPaddress (moduleEntry 22)

Provides the IP address of the VLAN router module (for the Catalyst 5000). If the module has a separate receive IP address, it is reported here; otherwise, the value is 0000000H.

Syntax: DisplayString

Access: Read-only

moduleIPvlan (moduleEntry 23)

Provides the VLAN IP address of the VLAN router module (for the Catalyst 5000). If the moduleIpAddress is valid, this object reports to the VLAN that this IP address is accessible; otherwise, the value is 0.

Syntax: DisplayString

Access: Read-only

End of Table

Port Group

The Port group provides information for a particular port on a module, such as port location, port name (as designated by the network administrator), port type, operational status, mode (half- or full-duplex), and port security.

Implementation of the Port group is mandatory for all Cisco Workgroup Stack products.

portTable (portGrp 1)

Contains a list of port entries. The number of entries is determined by the number of modules in the chassis and the number of ports on each module and includes the following variables: *portModuleIndex, portIndex, portCrossIndex, portName, portType, portOperStatus, portCrossGroupIndex, portAdditionalStatus, portAdminSpeed, portDuplex, portIfIndex,* and *portSpantreeFastStart*.

Syntax: SEQUENCE OF PortEntry

Access: Not accessible

portEntry (portTable 1)

Contains information for a particular port on a module.

Syntax: PortEntry

Access: Not accessible

portModuleIndex (portEntry 1)

Indicates an index value that uniquely identifies the module where this port is located. The chassis slot number which the module is plugged into determines the value. Valid entries are 1 to the value of chassisNumSlots.

Syntax: Integer (1..16)

Access: Read-only

portIndex (portEntry 2)

Indicates an index value that uniquely identifies this port within a module. The location of the port on the module determines the value. Valid entries are 1 to the value of moduleNumPorts for this module.

Syntax: Integer (1..255)

Access: Read-only

portCrossIndex (portEntry 3)

Indicates a cross-reference to the port's index within another MIB group. The value is dependent on the type of port. For an FDDI port, the value corresponds to the snmpFddiPORTIndex.

Syntax: Integer (1..4080)

Access: Read-only

portName (portEntry 4)

Specifies a descriptive string used by the network administrator to name the port.

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

portType (portEntry 5)

Indicates the type of physical layer medium-dependent interface on the port.

Syntax: Integer {

other (1)	None of the following
cddi (2)	CDDI (unshielded twisted-pair [UTP] FDDI)
fddi (3)	Multimode fiber FDDI
tppmd (4)	ANSI standard UTP FDDI

portType (portEntry 5)—Continued

mlt3 (5)	MLT-3 UTP FDDI
sddi (6)	Shielded twisted-pair (STP) FDDI
smf (7	Single-mode fiber FDDI
e10BaseT (8)	UTP Ethernet
e10BaseF (9)	Multimode fiber Ethernet
scf (10)	Small-connector fiber FDDI
e100BaseTX (11)	UTP Fast Ethernet (Catalyst 5000 series)
e100BaseT4 (12)	UTP Fast Ethernet (Catalyst 3000 series)
e100BaseF (13)	Multimode fiber Fast Ethernet
atmOc3mmf (14)	Multimode fiber OC-3 ATM
atmOc3smf (15)	Single-mode fiber OC-3 ATM
atmOc3utp (16)	UTP OC-3 ATM
e100BaseFsm (17)	Single-mode fiber Fast Ethernet
e10a100BaseTX (18)	10/100 UTP Ethernet (Catalyst 3000 series/5000 series)
mii (19)	MII Ethernet
vlanRouter (20)	VLAN router module (for the Catalyst 5000 series)

Access: Read-only

portOperStatus (portEntry 6)

Indicates the current operational status of the port.

Syntax: Integer {

other (1)	None of the following
ok (2)	Status satisfactory

portOperStatus (portEntry 6)—Continued

minorFault (3) Minor problem

majorFault (4) Major problem

Access: Read-only

portCrossGroupIndex (portEntry 7)

Indicates a cross-reference to another MIB group for this port. The value is dependent on the type of port. For an FDDI port, the value corresponds to the snmpFddiPORTSMTIndex.

Syntax: Integer (1..16)

Access: Read-only

portAdditionalStatus (portEntry 8)

Provides additional status information for the port. The value is a sum. It initially takes the value zero, then for each state that is true, two raises to a power and is added to the sum. The following table lists the powers:

State	Power
Transmit	0
Receive	1
Collision	2

portAdditionalStatus (portEntry 8)—Continued

Transmit state indicates that at least one packet was transmitted by the port in the last polling period. Receive state indicates that at least one packet was received by the port in the last polling period. Collision state indicates that at least one collision was detected on the port in the last polling period.

Note If a state is not applicable to a particular port, its value is always false for that port.

Syntax: Integer (0..7)

Access: Read-only

portAdminSpeed (portEntry 9)

Specifies the desired speed of the port in bits per second. The current operational speed of the port can be determined from ifSpeed.

Syntax: Integer {

autoDetect (1)

s10000000 (10000000)

s100000000 (100000000)

s155000000 (155000000)

s400000000 (400000000) for the VLAN router module (for the Catalyst 5000 series)

Access: Read-write

portDuplex (portEntry 10)

Specifies whether the port is operating in half-duplex or full-duplex mode.

Syntax: Integer {

half (1)	Operating in half-duplex mode
full (2)	Operating in full-duplex mode

Access: Read-write

portIfIndex (portEntry 11)

Indicates the value of the instance of the ifIndex object, defined in MIB-II, for the interface corresponding to this port.

Syntax: Integer (1..4294967295)

Access: Read-only

portSpantreeFastStart (portEntry 12)

Enables or disables spanning-tree fast start mode. A port with fast start enabled is immediately put in spanning-tree forwarding state on link up, rather than starting in blocking state, which is the normal operation. Fast start enabled is useful when the port is known to be connected to a single station that has problems waiting for the normal spanning-tree operation to put the port in forwarding state.

Syntax: Integer {

enabled (1)	Operating in spanning-tree fast start mode
disabled (2)	Not operating in spanning-tree fast start mode (default)

Access: Read-write

End of Table

Trivial File Transfer Protocol Group

The Trivial File Transfer Protocol (TFTP) group manages and controls products that implement TFTP upload/download functions, such as source/destination host for the transfer, TFTP transfer filename, code/configuration transfer, software or firmware transfer, and TFTP action results.

Implementation of the TFTP group is mandatory for all Cisco Workgroup Stack products that implement TFTP upload/download functions.

tftpHost (tftpGrp 1)

Indicates the name of the source/destination host for the TFTP transfer.

Syntax: DisplayString (SIZE (0..64))

Access: Read-write

tftpFile (tftpGrp 2)

Indicates the name of the file for TFTP transfer.

Syntax: DisplayString (SIZE (0..64))

Access: Read-write

tftpModule (tftpGrp 3)

Specifies which module's code/configuration is being transferred.

Syntax: Integer (0..16)

Access: Read-write

If set to 0, the system recognizes the image type the given file contains and downloads it to all modules of the appropriate type in the chassis.

tftpAction (tftpGrp 4)

Setting this object to one of the acceptable values initiates the requested action using the information given in tftpHost, tftpFile, and tftpModule. Setting this object to any other value results in an error.

Syntax: Integer {

downloadConfig (2)	Receive configuration from host/file
uploadConfig (3)	Send configuration to the host/file
downloadSw (4)	Receive software image from the host/file
uploadSw (5)	Send software image to the host/file
downloadFw (6)	Receive firmware image from the host/file
uploadFw (7)	Send firmware image to the host/file

Access: Read-write

tftpResult (tftpGrp 5)

Contains the result of the last TFTP action request.

Syntax: Integer {

inProgress (1)

success (2)

noResponse (3)

tooManyRetries (4)

noBuffers (5)

noProcesses (6)

badChecksum (7)

badLength (8)

tftpResult (tftpGrp 5)—Continued

badFlash (9)

serverError (10)

userCanceled (11)

wrongCode (12)

Access: Read-only

Monitor Group

The Monitor group manages and controls variables that implement port monitoring functions, such as monitoring port location, monitoring destination port location, packet type to be monitored, and enabling port monitoring.

Implementation of the Monitor group is mandatory for all Cisco Workgroup Stack products that implement port monitoring functions.

monitorSourceModule (monitorGrp 1)

Specifies an index value that uniquely identifies the module where the monitoring source port is located. A value of 0 indicates that the monitorSourcePort is really a source VLAN number.

Syntax: Integer (0..16)

Access: Read-write

monitorSourcePort (monitorGrp 2)

Specifies an index value that uniquely identifies the monitoring source port within a module or the monitoring source VLAN.

Syntax: Integer (0..1023)

Access: Read-write

monitorDestinationModule (monitorGrp 3)

Specifies an index value that uniquely identifies the module where the monitoring destination port is located.

Syntax: Integer (1..16)

Access: Read-write

monitorDestinationPort (monitorGrp 4)

Specifies an index value that uniquely identifies the monitoring destination port within a module.

Syntax: Integer (1..255)

Access: Read-write

monitorDirection (monitorGrp 5)

Specifies the type of packets to be monitored at the source port.

Syntax: Integer {

transmit (1)

receive (2)

transmitAndReceive (3) (default)

Access: Read-write

monitorEnable (monitorGrp 6)

Enables or disables port monitoring.

Syntax: Integer {

enabled (1) Port monitoring is enabled.

disabled (2) Port monitoring is disabled (default).

Access: Read-write

VLAN Group

The VLAN group manages and controls variables that implement VLAN functions, such as port location, port VLAN information, list of port entries, priority level used to access the switching media, and operational status.

Implementation of the VLAN group is mandatory for all Cisco Workgroup Stack products that implement VLAN functions.

Note vlanGrp 1 is not used.

vlanTable (vlanGrp 2)

Contains a list of VLAN entries. The number of entries is determined by the number of VLANs supported by the system. The following variables are available: vlanIndex and vlanSpantreeEnable.

Syntax: SEQUENCE OF VlanEntry

Access: Not accessible

vlanEntry (vlanTable 1)

Contains information for a particular VLAN.

Syntax: VlanEntry

Access: Not accessible

vlanIndex (vlanEntry 1)

Indicates an index value that uniquely identifies the VLAN associated with this information.

Syntax: Integer (0..1023)

Access: Read-only

vlanSpantreeEnable (vlanEntry 2)

Enables or disables Spanning-Tree Protocol for this VLAN.

Syntax: Integer {

enabled (1) Spanning-Tree Protocol is enabled (default).

disabled (2) Spanning-Tree Protocol is disabled.

Access: Read-write

End of Table

vlanPortTable (vlanGrp 3)

Contains a list of VLAN port entries. The number of entries is determined by the number of modules in the chassis and the number of ports on each module. The following variables are available: *vlanPortModule, vlanPort, vlanPortVlan, vlanPortIslVlansAllowed, vlanPortSwitchLevel, vlanPortIslAdminStatus, vlanPortIslOperStatus, vlanPortIslPriorityVlans, vlanPortAdminStatus,* and *vlanPortOperStatus*.

Syntax: SEQUENCE OF VlanPortEntry

Access: Not accessible

vlanPortEntry (vlanPortTable 1)

Contains VLAN information for a particular port on a module.

Syntax: VlanPortEntry

Access: Not accessible

vlanPortModule (vlanPortEntry 1)

Indicates an index value that uniquely identifies the module where this port is located (see portModuleIndex).

Syntax: Integer (1..16)

Access: Read-only

vlanPort (vlanPortEntry 2)

Indicates an index value that uniquely identifies this port within a module (see portIndex).

Syntax: Integer (1..255)

Access: Read-only

vlanPortVlan (vlanPortEntry 3)

Specifies the VLAN to which this port belongs.

Syntax: Integer (0..1023)

Access: Read-write

Note vlanPortEntry4 is not used.

vlanPortIslVlansAllowed (vlanPortEntry 5)

Indicates which VLANs are allowed on this Inter-Switch Link (ISL). It is an octet string value with bits set to indicate allowed VLANs. It can be interpreted as a sum of f(x) as x goes from 0 to 1023, where f(x) = 0 for VLAN x not allowed and f(x) = exp(2, x) for VLAN x allowed. If all bits are 0 or the octet string is zero length, the port is not operating as an Inter-Switch Link.

Syntax: OCTET STRING (SIZE (1..128))

Access: Read-write

vlanPortSwitchLevel (vlanPortEntry 6)

Indicates the priority level the port uses to access the switching media.

Syntax: Integer {

normal (1)

high (2) (default)

Access: Read-write

vlanPortIslAdminStatus (vlanPortEntry 7)

Indicates the administrative status set on the trunk port. The operational status indicates whether the port is actually trunking or not. If the status is set to on (1) or off (2), the port is permanently set to be a trunk or nontrunk, respectively. When the status is set to desirable (3), the port initiates a request to become a trunk, and it becomes a trunk if another device's port on that link agrees. When the status is set to auto (4), the port will become a trunk if it receives a request to become a trunk.

Note The status for 802.10-capable ports can only be either on (1) or off (2), and the default is off (2). The status for ISL-capable ports can be any of the four, and any change in status starts the negotiation process. For ISL-capable ports, the default is auto (4).

Syntax: Integer {

on (1)	The port is permanently set to be a trunk.
off (2)	The port is permanently set to be a nontrunk.
desirable (3)	The port initiates a request to become a trunk, and it will become a trunk if another device's port on that link agrees.
auto (4)	The port becomes a trunk if it receives a request to become a trunk.

Access: Read-write

vlanPortIslOperStatus (vlanPortEntry 8)

Indicates if the port is actually trunking or not. In the case of ISL-capable ports, the status depends on the success or failure of the negotiation process initiated by the port to become a trunk or nontrunk. In the case of 802.10-capable ports, it is directly related to the on/off administrative status.

Syntax: Integer {

trunking (1) The port is trunking.

notTrunking (2) The port is not trunking.

Access: Read-only

vlanPortIslPriorityVlans (vlanPortEntry 9)

Specifies an indication of which VLANs have a better dot1dStpPortPriority value. This object can be used to perform load balancing on ISLs via Spanning-Tree. An ISL has two dot1dStpPortPriority values which are shared by all the VLANs on the link. The VLANs indicated by this object have priority over the other VLANs on the link.

This is an octet string value with bits set to indicate priority VLANs. It can be interpreted as a sum of f(x) as x goes from 0 to 1023, where f(x) = 0 for a VLAN x which does not have priority and f(x) = exp(2, x) for a VLAN x which has priority.

Setting the dot1dStpPortPriority value for any of the VLANs indicated by this object causes the dot1dStpPortPriority value for all the VLANs indicated by this object to be set to the same value. Setting the dot1dStpPortPriority value for any other VLAN causes the dot1dStpPortPriority value for all other VLANs to be set to the same value.

Syntax: OCTET STRING (SIZE (0..128))

Access: Read-write

vlanPortAdminStatus (vlanPortEntry 10)

Indicates the method in which the port is assigned to a VLAN (statically or dynamically). When it is set to dynamic, the needed information is accessed from one of the VLAN Membership Policy Servers (VMPS) specified in the vmpsTable. Default value is static(1).

Note The vlanPortAdminStatus cannot be set to dynamic (2) for a port which has portSecurityAdminStatus set to enabled (1) or for a port which currently has a vlanPortIslOperStatus of trunking (1).

Syntax: Integer {

static (1)	The port is assigned to a VLAN statically (default).
dynamic (2)	The port is assigned to a VLAN dynamically.

Access: Read-write

vlanPortOperStatus (vlanPortEntry 11)

Indicates the current VLAN status of the port. A status of inactive (1) indicates that a dynamic port does not yet have a VLAN assigned or that a static or dynamic port has been assigned a VLAN that is not currently active. A status of active (2) indicates that the currently assigned VLAN is active. A status of shutdown (3) indicates that the port has been shut down as a result of a VMPS response on a dynamic port.

Syntax: Integer {

inactive (1)	A dynamic port does not yet have a VLAN assigned, or a static or dynamic port has been assigned a VLAN that is not currently active.
active (2)	The currently assigned VLAN is active.
shutdown (3)	The port has been shut down as a result of a VMPS response on a dynamic port.

End of Table

vmpsTable (vlanGrp 4)

Contains a list of VMPS IP addresses; maximum three addresses. The following variables are available: *vmpsAddr, vmpsType.*

Syntax: SEQUENCE OF VmpsEntry

Access: Not accessible

vmpsEntry (vmpsTable 1)

Contains a list of VMPS entries.

Syntax: VmpsEntry

Access: Not accessible

vmpsAddr (vmpsEntry 1)

The VMPS IP address. To configure the internal VMPS, use the same IP address as specified in sysIpAddr.

Syntax: IpAddress

Access: Read-only

vmpsType (vmpsEntry 2)

To remove an entry from the table, set this object to invalid (1). To add a new entry to the vmpsTable, set this object to primary (2) or other (3) for an IP address which is not already in the table. The primary entry will be used first, if it is reachable. Otherwise, one of the other entries will be used. Setting one entry to primary (2) causes any previous primary entry to change to other (3).

vmpsType (vmpsEntry 2)—Continued

Syntax: Integer {

invalid (1)	Remove this entry
primary (2)	The primary entry
other (3)	A lower priority entry

Access: Read-write

End of Table

vmpsAction (vlanGrp 5)

When read, this object returns the result of the last action requested: other (1), inProgress (2), success (3), noResponse (4), noPrimaryVmps (5), noDynamicPort (6), or noHostConnected (7).

Setting this object to reconfirm (8) causes the switch to contact the VMPS immediately to reconfirm the current VLAN assignments for all dynamic ports on the switch. Normally VLAN assignments for dynamic ports are reconfirmed once an hour.

Syntax: Integer {

other (1)	None of following (read-only)
inProgress (2)	Read-only
success (3)	Read-only
noResponse (4)	Read-only
noPrimaryVmps (5)	No VMPS configured (read-only)
noDynamicPort (6)	No dynamic ports configured (read-only)
noHostConnected (7	No hosts on dynamic ports (read-only)
reconfirm (8)	Write-only

Access: Read-write

vmpsAccessed (vlanGrp 6)

The IP address of the last VMPS accessed. If there was no response from the last VMPS request, the value returned is 0.

Syntax: IpAddress

Access: Read-only

Security Group

The Security group controls and manages variables that pertain to port security functions, such as listing security information for a specific port, port security entries, module index, port index, and enabling source MAC address monitoring. Implementation of the Security group is optional, but within the group all the elements are mandatory. If the Security feature is implemented, the entire group must be implemented.

portSecurityTable (securityGrp 1)

Contains a list of port security entries. The number of entries is determined by the number of ports in the system that support the Security feature and includes the following variables: *portSecurityModuleIndex*, *portSecurityPortIndex*, *portSecurityAdminStatus*, *portSecurityOperStatus*, *portSecurityLastSrcAddr*, and *portSecuritySecureSrcAddr*.

Syntax: SEQUENCE OF PortSecurityEntry

Access: Not accessible

portSecurityEntry (portSecurityTable 1)

Contains security information for a particular port.

Syntax: PortSecurityEntry

Access: Not accessible

portSecurityModuleIndex (portSecurityEntry 1)

Provides an index value that uniquely identifies the module where this port is located (see portModuleIndex).

Syntax: Integer (1 .. 16)

Access: Read-only

portSecurityPortIndex (portSecurityEntry 2)

Provides an index value that uniquely identifies this port within a module (see portIndex).

Syntax: Integer (1..255)

Access: Read-only

portSecurityAdminStatus (portSecurityEntry 3)

Monitors source MAC addresses for all packets received on the port when security is enabled. If an address is detected that does not match the portSecuritySecureSrcAddr, the port is shut down and a linkDown trap is sent.

Syntax: Integer {

enabled (1)	Source MAC addresses are monitored for all packets received on the port.
disabled (2)	Source MAC addresses are not monitored for all packets received on the port (default).

Access: Read-write

portSecurityOperStatus (portSecurityEntry 4)

Indicates whether the port has been shut down as a result of an insecure address being detected on a secure port.

Syntax: Integer {

notShutdown (1)	Port has not shut down.
shutdown (2)	Port has been shut down as a result of an insecure address being detected on a secure port.

Access: Read-only

portSecurityLastSrcAddr (portSecurityEntry 5)

Indicates the last source MAC address in a receive packet seen on the port.

Syntax: OCTET STRING (SIZE (6))

Access: Read-only

portSecuritySecureSrcAddr (portSecurityEntry 6)

Indicates the address to be compared with source MAC addresses of received packets when the portSecurityAdminStatus is enabled (1). Setting this value to 0.0.0.0.0.0 puts the port in learning mode so that the next source MAC address received by the port becomes the portSecuritySecureSrcAddr.

Syntax: OCTET STRING (SIZE (6))

Access: Read-write

End of Table

Multicast Group

The Multicast group controls and manages variables that pertain to multicast functions, such as lists multicast router port entries, provides multicast router information per port or module, sets the presence of an IP multicast router on this port to be determined statically or dynamically, and sets whether Cisco Group Management Protocol (CGMP) is enabled on the device or not.

Implementation of the Multicast group is optional, but within the group all the elements are mandatory.

mcastRouterTable (multicastGrp 1)

Contains a list of multicast router port entries. The number of entries is determined by the number of ports in the system and includes the following variables: *mcastRouterModuleIndex, mcastRouterPortIndex, mcastRouterAdminStatus,* and *mcastRouterOperStatus*.

Syntax: SEQUENCE OF McastRouterEntry

Access: Not accessible

mcastRouterEntry (mcastRouterTable 1)

Contains multicast router information for a particular port.

Syntax: McastRouterEntry

Access: Not accessible

mcastRouterModuleIndex (mcastRouterEntry 1)

Provides an index value that uniquely identifies the module where this port is located (see portModuleIndex).

Syntax: Integer (1..16)

Access: Read-only

mcastRouterPortIndex (mcastRouterEntry 2)

Provides an index value that uniquely identifies this port within a module (see portIndex).

Syntax: Integer (1..255)

Access: Read-only

mcastRouterAdminStatus (mcastRouterEntry 3)

Indicates whether the presence of an IP multicast router on this port is to be determined statically or dynamically.

Syntax: Integer {

routerPresent (1)	The router presence is configured statically as present.
dynamic (3)	The router presence is learned dynamically (default).

Access: Read-write

mcastRouterOperStatus (mcastRouterEntry 4)

Indicates whether an IP multicast router is present on this port.

Syntax: Integer {

routerPresent (1)	An IP multicast router is present.
noRouter (2)	An IP multicast router is not present.

Access: Read-only

End of Table

mcastEnableCgmp (multicastGrp 2)

Enables or disables Cisco Group Management Protocol (CGMP) on the device. When CGMP is enabled in conjunction with Cisco routers running CGMP, only the required ports will participate in IP multicast groups.

Syntax: Integer {

enabled (1)	Cisco Group Management Protocol is enabled.
disabled (2)	Cisco Group Management Protocol is disabled (default).

Access: Read-write

Domain Naming System Group

The Domain group controls and manages variables that pertain to domain functions, such as enables or disables the Domain Naming System (DNS) feature, adds or removes servers, and specifies the domain name.

Implementation of the DNS group is optional, but within the group all the elements are mandatory. If DNS features are implemented, the entire group must be implemented.

dnsEnable (dnsGrp 1)

Enables or disables the DNS feature.

Syntax: Integer {

enabled (1)	DNS feature is enabled.
disabled (2)	DNS feature is disabled (default).

Access: Read-write

dnsServerTable (dnsGrp 2)

Contains a list of a maximum of three DNS servers and includes the following variables: *dnsServerAddr* and *dnsServerType*.

Syntax: SEQUENCE OF DnsServerEntry

Access: Not accessible

dnsServerEntry (dnsServerTable 1)

Contains a DNS server table entry.

Syntax: DnsServerEntry

Access: Not accessible

dnsServerAddr (dnsServerEntry 1)

Provides the IP address of a DNS server.

Syntax: IpAddress

Access: Read-only

dnsServerType (dnsServerEntry 2)

Removes, adds, or changes the priority level of a dnsServerTable entry. To remove an entry from the dnsServerTable, set this object to invalid (1). To add a new entry to the dnsServerTable, set this object to primary (2) or other (3) for an IP address that is not already in the table. If it is reachable, the primary entry is used first. Otherwise, one of the other entries is used. Setting one entry to primary (2) causes any previous primary entry to change to other (3).

Syntax: Integer {

invalid (1)	Remove this entry.
primary (2)	The primary entry.
other (3)	A lower priority entry.

Access: Read-write

End of Table

dnsDomainName (dnsGrp 3)

Specifies the DNS domain name.

Syntax: DisplayString (SIZE (0..255))

Access: Read-write

System Log Information Group

The System Log group controls and manages variables that pertain to System Log functions, such as list system log servers, provide system log IP address, add or remove a system log server, and indicate where system log messages are to be sent (console or system log server).

Implementation of the syslog group is optional, but within the group all the elements are mandatory. If the syslog feature is implemented, the entire group must be implemented.

syslogServerTable (syslogGrp 1)

Contains a list of system log servers (maximum of three) and includes the following variables: *syslogServerAddr* and *syslogServerType*.

Syntax: SEQUENCE OF SyslogServerEntry

Access: Not accessible

syslogServerEntry (syslogServerTable 1)

Provides a system log server table entry.

Syntax: SyslogServerEntry

Access: Not accessible

syslogServerAddr (syslogServerEntry 1)

Provides the IP address of a system log server.

Syntax: IpAddress

Access: Read-only

syslogServerType (syslogServerEntry 2)

Adds or removes syslogServerTable entries. To add a new entry into syslogServerTable, set this object to valid (1) for an IP address not already in the table. To remove an entry from the syslogServerTable, set to invalid (2).

Syntax: Integer {

valid (1)	Add this entry.
invalid (2)	Remove this entry.

Access: Read-write

End of Table

syslogConsoleEnable (syslogGrp 2)

Indicates whether the system log messages should be sent to console.

Syntax: Integer {

enabled (1)	System log messages are sent to console.
disabled (2)	System log messages are not sent to console (default).

Access: Read-write

syslogHostEnable (syslogGrp 3)

Indicates whether the system log messages should be sent to syslog servers.

Syntax: Integer {

enabled (1)	System log messages are sent to syslog servers.
disabled (2)	System log messages are not sent to syslog servers (default).

Access: Read-write

syslogMessageControlTable (syslogGrp 4)

This table contains the information about what system log messages should be sent to syslog host, console, login session, and/or logged into the internal buffer and includes the following variables: *syslogMessageFacility* and *syslogMessageSeverity.*

Syntax: SEQUENCE OF SyslogMessageControlEntry

Access: Not accessible

syslogMessageControlEntry (syslogMessageControlTable 1)

Provides a system log message control table entry.

Syntax: SyslogMessageControlEntry

Access: Not accessible

syslogMessageFacility (syslogMessageControlEntry 1)

Provides the system log message facility.

Syntax: Integer {

cdp (1)

cgmp (2)

disl (3)

dvlan (4)

earl (5)

fddi (6)

ip (7)

pruning (8)

snmp (9)

spantree (10)

system (11)

syslogMessageFacility (syslogMessageControlEntry 1)—Continued

tac (12)

tcp (13)

telnet (14)

tftp (15)

vtp (16)

vmps (17)

Access: Read-only

syslogMessageSeverity (syslogMessageControlEntry 2)

Indicates the system log message severity.

Syntax: Integer {

emergencies (1)

alerts (2)

critical (3)

errors (4)

warnings (5)

notification (6)

informational (7)

debugging (8)

Access: Read-write

End of Table

Network Time Protocol Group

The Network Time Protocol (NTP) group controls and manages variables that pertain to NTP functions, such as indicate whether the Catalyst 5000 series switch should act as a broadcast or NTP client or not, set NTP broadcast round trip time (in microseconds), list NTP IP address, set the system to change for daylight saving time, and set time zone.

Implementation of the NTP group is optional, but within the group all the elements are mandatory. If the NTP feature is implemented, the entire group should be implemented.

ntpBcastClient (ntpGrp 1)

Enables or disables the broadcast client feature.

Syntax: Integer {

enabled (1)	Catalyst 5000 acts as a broadcast client.
disabled (2)	Catalyst 5000 does not act as a broadcast client (default).

Access: Read-write

ntpBcastDelay (ntpGrp 2)

Estimates the round trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Syntax: Integer (1..999999)

Access: Read-write

Access: 3000 (3000)

ntpClient (ntpGrp 3)

Enables or disables the NTP feature.

Syntax: Integer {

enabled (1) Catalyst 5000 acts as an NTP client.

disabled (2) Catalyst 5000 does not act as an NTP client (default).

Access: Read-write

ntpServerTable (ntpGrp 4)

Contains a list of NTP server entries. This table lists a maximum of ten entries and contains the following variables: *ntpServerAddress* and *ntpServerType*.

Syntax: SEQUENCE OF NtpServerEntry

Access: Not accessible

ntpServerEntry (ntpServerTable 1)

Contains NTP information for a particular entry.

Syntax: NtpServerEntry

Access: Not accessible

ntpServerAddress (ntpServerEntry 1)

Contains NTP Server's IP address.

Syntax: IpAddress

Access: Read-only

ntpServerType (ntpServerEntry 2)

Adds or removes entries to the ntpServerTable. To add a new entry to the ntpServerTable, set this object to valid (1) for an IP address that is not in the table. To remove an entry from the table, set this object to invalid (2).

Syntax: Integer {

valid (1)	Add this entry.
invalid (2)	Remove this entry.

Access: Read-write

End of Table

ntpSummertimeStatus (ntpGrp 5)

Sets the clock ahead or behind one hour respectively (daylight saving time in USA). This command becomes active only in the summer time.

Syntax: Integer {

enabled (1)	Sets the clock ahead 1 hour.
disabled (2)	Sets the clock behind 1 hour (default).

Access: Read-write

ntpSummerTimezoneName (ntpGrp 6)

Provides summer time zone name for display purposes.

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

ntpTimezoneName (ntpGrp 7)

Provides time zone name for display purposes.

Syntax: DisplayString (SIZE (0..20))

Access: Read-write

ntpTimezoneOffsetHour (ntpGrp 8)

Provides time offset (in hours) from Greenwich Mean Time.

Syntax: Integer (-12..12)

Access: Read-write

ntpTimezoneOffsetMinute (ntpGrp 9)

Provides time offset (in minutes) from Greenwich Mean Time.

Syntax: Integer (0..59)

Access: Read-write

Terminal Access Controller Access Control System Group

The Terminal Access Controller Access Control System (TACACS) group controls and manages variables that pertain to TACACS functions, such as login parameter, encryption of packets passed between the TACACS+ server and the client, and IP address of a TACACS+ server.

Implementation of the TACACS group is optional, but within the group all the elements are mandatory. If the TACACS+ feature is implemented, the entire group must be implemented.

tacacsLoginAuthentication (tacacsGrp 1)

Indicates whether the login authentication using the TACACS+ feature is enabled or disabled.

Syntax: Integer {

enabled (1)	Login authentication using the TACACS+ feature is enabled.
disabled (2)	Login authentication is not using the TACACS+ feature (default).

Access: Read-write

tacacsEnableAuthentication (tacacsGrp 2)

Indicates whether the enable authentication using the TACACS+ feature is enabled or disabled.

Syntax: Integer {

enabled (1)	Authentication using the TACACS+ feature is enabled.
disabled (2)	Authentication using the TACACS+ feature is disabled (default).

Access: Read-write

tacacsLocalLoginAuthentication (tacacsGrp 3)

Indicates whether the login authentication using local password is enabled or disabled.

Syntax: Integer {

enabled (1) Login authentication using local password is enabled (default).

disabled (2) Login authentication using local password is disabled.

Access: Read-write

tacacsLocalEnableAuthentication (tacacsGrp 4)

Indicates whether the enable authentication using local password is enabled or disabled.

Syntax: Integer {

enabled (1) Authentication using local password is enabled (default).

disabled (2) Authentication using local password is disabled.

Access: Read-write

tacacsNumLoginAttempts (tacacsGrp 5)

Indicates the number of login attempts allowed before the system locks you out.

Syntax: Integer (1..10) (default is 3)

Access: Read-write

tacacsDirectedRequest (tacacsGrp 6)

Indicates whether the directed-request feature of TACACS+ is enabled or disabled.

Syntax: Integer {

enabled (1)

disabled (2) (default)

Access: Read-write

tacacsTimeout (tacacsGrp 7)

Indicates the duration in seconds to wait for a response from the TACACS+ server host.

Syntax: Integer (1..255) (default is 5)

Access: Read-write

Note *tacacsAuthKey* is only accessible when using the community string defined in sysCommunityRwa.

---

tacacsAuthKey (tacacsGrp 8)

Indicates the key used in encrypting the packets passed between the TACACS+ server and the client. This key must match the one configured on the server.

Syntax: DisplayString (SIZE (0..100)) (default is Null)

Access: Read-write

tacacsServerTable (tacacsGrp 9)

Contains a list of TACACS+ servers (maximum of three), and includes the following variables: *tacacsServerAddr* and *tacacsServerType*.

Syntax: SEQUENCE OF TacacsServerEntry

Access: Not accessible

tacacsServerEntry (tacacsServerTable 1)

Provides a TACACS+ server table entry.

Syntax: TacacsServerEntry

Access: Not accessible

tacacsServerAddr (tacacsServerEntry 1)

Indicates the IP address of a TACACS+ server.

Syntax: IpAddress

Access: Read-only

tacacsServerType (tacacsServerEntry 2)

Removes or adds a tacacsServerEntry. To remove an entry from the table, set this object to invalid (1). To add a new entry to the tacacsServerTable, set this object to primary (2) or other (3) for an IP address not already in the table. If it is reachable, the primary entry is used first. Otherwise, one of the other entries is used. Setting one entry to primary (2) causes any previous primary entry to change to the other (3).

Syntax: Integer {

invalid (1)	Remove this entry.
primary (2)	The primary entry.
other (3	A lower priority entry.

Access: Read-write

End of Table

IP Permit List Group

The IP Permit List group controls and manages variables that pertain to IP permit list functions, such as access level and IP address of an IP Permit host.

Implementation of the IP Permit List group is optional, but within the group all the elements are mandatory. If the IP Permit List feature is implemented, the entire group must be implemented.

ipPermitEnable (ipPermitListGrp 1)

Indicates whether the IP permit feature is enabled or disabled.

Syntax: Integer {

enabled (1)

disabled (2) (default)

Access: Read-write

ipPermitListTable (ipPermitListGrp 2)

Contains a list of a maximum of ten IP addresses with net masks of IP permit hosts. If ipPermitEnable is enabled, the system only accepts the inbound Telnet and SNMP access from the configured hosts in this table. The following variables are included: *ipPermitAddress, ipPermitMast, ipPermitType*.

Syntax: SEQUENCE OF IpPermitListEntry

Access: Not accessible

ipPermitListEntry (IpPermitListTable 1)

Provides an IP permit list table entry.

Syntax: IpPermitListEntry

Access: Not accessible

ipPermitAddress (ipPermitListEntry 1)

Indicates the IP address of an IP permit host.

Syntax: IP address

Access: Read-only

ipPermitMask (ipPermitListEntry 2)

Indicates the IP net mask of an IP permit host.

Syntax: IP address

Access: Read-only

ipPermitType (ipPermitListEntry 3)

To add a new entry to the ipPermitListTable for an IP address and net mask which are not in the table, set this object to valid (1). Setting to invalid (2) removes the corresponding entry from the ipPermitListTable.

Syntax: Integer {

valid (1)	Remove this entry
invalid (2)	Add this entry

Access: Read-write

End of Table

ipPermitDeniedListTable (ipPermitListGrp 3)

Contains a list of the most recently denied addresses with the access type; a maximum of ten IP addresses can be displayed. The following variables are included: *ipPermitDeniedAddress, ipPermitDeniedAccess, ipPermitDeniedTime.*

Syntax: SEQUENCE OF IpPermitDeniedListEntry

Access: Not accessible

ipPermitDeniedListEntry (ipPermitDeniedListTable 1)

Provides an IP permit denied list table entry.

Syntax: ipPermitDeniedListEntry

Access: Not accessible

ipPermitDeniedAddress (ipPermitDeniedListEntry 1)

Indicates the IP address of an IP permit denied access.

Syntax: IP address

Access: Read-only

ipPermitDeniedAccess (ipPermitDeniedListEntry 2)

Indicates the denied access type.

Syntax: Integer {

telnet (1)

snmp (2)

Access: Read-only

ipPermitDeniedTime (ipPermitDeniedListEntry 3)

Indicates the time (in hundredths of a second) since the IP permit denied access happened.

Syntax: TimeTicks {

Access: Read-only

End of Table

Port Channel Group

The Port Channel group controls and manages variables that pertain to Ethernet Channeling functions, such as port selection and status.

Implementation of the Port Channel group is optional, but within the group all the elements are mandatory. If the Port Channel feature is implemented, the entire group must be implemented.

portChannelTable (portChannelGrp 1)

Contains a list of port channel entries, and includes the following variables: *portChannelModuleIndex, portChannelPortIndex, portChannelPorts, portChannelAdminStatus, portChannelOperStatus*.

Syntax: SEQUENCE OF PortChannelEntry

Access: Not accessible

portChannelEntry (portChannelTable 1)

Provides an entry containing information for a particular port on a module.

Syntax: PortChannelEntry

Access: Not accessible

portChannelModuleIndex (portChannelEntry 1)

Indicates an index value that uniquely identifies the module where this port is located. The value is determined by the chassis slot number in which the module is located.

Syntax: Integer (1..16)

Access: Read-only

portChannelPortIndex (portChannelEntry 2)

Indicates an index value that uniquely identifies this port within a module.

Syntax: Integer (1..255)

Access: Read-only

portChannelPorts (portChannelEntry 3)

Indicates the set of ports on a module which are channeled together. Each octet within the value of this object specifies a set of eight ports, with the first octet specifying ports 1 through 8, the second octet specifying ports 9 through 16, and so forth. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port. Therefore, each port is represented by a single bit within the value of this object. If given a value of 1, the port is included in the set of channel ports. The default is a string which only has a value of 1 on its own port.

Syntax: OCTET STRING (SIZE [0..8])

Access: Read-write

portChannelAdminStatus (portChannelEntry 4)

Indicates the administrative status set on the channeled ports. If status is set to on (1), channeling is enabled; if set to off (2), channeling is disabled.

Syntax: Integer {

on (1)	Channeling is enabled
off (2)	Channeling is disabled (default)

Access: Read-write

portChannelOperStatus (portChannelEntry 5)

Indicates whether the current channeling operational status of a port is channeling or not channeling.

Syntax: Integer {

channelling (1)	Port is channeling
notchannelling (2)	Port is not channeling

Access: Read-only

Spanning-Tree Status Group

The Spanning-Tree Status group provides VLAN information. Implementation of the Spanning-Tree Status group is voluntary for all Cisco Workgroup Stack products.

cvbStpTable (cvbStp 1)

This table contains device Spanning-Tree Protocol (STP) status information for each VLAN, and includes the following variable: *cvbStpForwardingMap*.

Syntax: SEQUENCE OF CiscoVlanStpEntry

Access: Not accessible

cvbStpEntry (cvbStpTable 1)

Device STP status for a specified VLAN.

Syntax: CiscoVlanStpEntry

Access: Not accessible

Note cvbStpEntry 1 is not used.

cvbStpForwardingMap (cvbStpEntry 2)

An indication of which ports are forwarding by spanning tree for the specified VLAN. The octet string contains one bit per port on the bridge for the specified VLAN.

Each bit within the octet string represents one port of the device. The ordering of ports represented within the octet string is in the same order as in the RFC 1493 dot1dStpPortTable.

The bit value interpretation related to RFC 1493 dot1dStpPortState values is as follows:

- 1 = forwarding
- 0 = disabled, blocking, listening, learning, broken, or nonexistent

Syntax: OCTET STRING (SIZE (0..128))

Access: Read-only